AF/2876/$ IFW

PATENT

01AB082

CERTIFICATE OF MAILING

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-14501.

5-17-04
Date:

Himanshu S. Amin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant(s): Joseph Lenner

Serial No: 09/938,227

Filing Date: August 23, 2001

Examiner: Jamara Alzaida Franklin

Art Unit: 2876

Title: ELECTRONIC LOCKOUT/TAGOUT SYSTEMS

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Applicant submits this brief in triplicate in connection with an appeal of the above-identified patent application. Please charge $330.00 for the fee associated with this brief to Deposit Account No. 50-1063[ALBRP230US].

05/25/2004 DEMMANU1 00000126 501063 09938227
01 FC:1402 330.00 DA

I. Real Party in Interest (37 C.F.R. §1.192(c)(1))

The real party in interest in the present appeal is Rockwell Automation Technologies, Inc., the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §1.192(c)(2))

Appellants, appellant's legal representatives, and/or the assignee of the present application are not aware of any appeals or interferences which will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §1.192(c)(3))

Claims 1-34 are pending in the subject application. The rejection of claims 1-34 is appealed.

IV. Status of Amendments (37 C.F.R. §1.192(c)(4))

No claim amendments have been entered subsequent the Final Office Action.

V. Summary of Invention (37 C.F.R. §1.192(c)(5))

The present invention provides a system that facilitates electronic disablement of dangerous equipment through electronic keys, an electronic key reader, a data analyzer and an electronically controlled disconnecting device. (p.2, ll.28-30). The system employs the electronic key reader to read information coded on an electronic key. (p.3, ll.4-8). Such information is related to a key holder and can include, for example, the task the key holder desires to perform, the approximate time estimated for the performance of the task, medical information associated with the key holder and other information. (p.3, ll.5-8). The key reader conveys the read information to the analyzer, which determines when and how to disable a piece of dangerous equipment. (p.3, ll.12-15). In addition, the analyzer conveys disconnect control information to the disconnecting device, which subsequently performs a disabling action on the dangerous equipment. (p.3, ll.22-25).

VI. Statement of the Issues (37 C.F.R. §1.192(c)(6))

A. Whether claims 1-3, 5-11 and 13-34 are unpatentable under 35 U.S.C. §102(b) as being anticipated by Castleman, *et al.* (US 5,508,691).

B. Whether claims 4 and 12 are unpatentable under 35 U.S.C. §103(a) over Castleman, *et al.* (US 5,508,691) in view of Mabuchi, *et al.* (US 6,417,760).

VII. Grouping of Claims (37 C.F.R. §1.192(c)(7))

For the purposes of this appeal only, the claims are grouped as follows:

claims 1-34 stand or fall together.

VIII. Argument (37 C.F.R. §1.192(c)(8))

A. Rejection of Claims 1-3, 5-11 and 13- 34 Under 35 U.S.C. §102(b)

Claims 1-3, 5-11 and 13-34 stand rejected under 35 U.S.C. §102(b) as being anticipated by Castleman, *et al.* (US 5,508,691). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Castleman, *et al.* does not teach or suggest ***each and every element*** of the subject claims.

i. *Applicable law*

> A single prior art reference anticipates a patent claim only if it expressly or inherently ***describes each and every limitation*** set forth in the patent claim. *Trintec Industries, Inc., v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 U.S.P.Q.2D 1597 (Fed. Cir. 2002). "A claim is anticipated only if ***each and every element*** as set forth in the claim is found, either expressly or inherently ***described*** in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The ***identical invention*** must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). (Emphasis added). (Emphasis added)

ii. *Castleman, et al. does not teach or suggest each and every element as recited in claims 1-3, 5-11 and 13-34; thus, Castleman, et al. does not anticipate the subject claims.*

The subject invention relates to controlling dangerous equipment based on an analysis of electronic data stored in an electronic key. Independent claims 1, 18, 23, 24, 29 and 33 recite similar limitations regarding employing an electronic key with electronic key data stored therein, wherein a data ***analyzer*** is employed to ***analyze*** the electronic key data and ***generate a control data based on the analysis*** that can be utilized to control dangerous equipment. Castleman, *et al.* does not teach or suggest such claimed aspects. Rather, Castleman, *et al.* discloses an electronic lock that ***compares*** a key code from an electronic key with pre-stored key codes in a lock to determine whether the read key code is authorized to toggle (open/close) the lock. Where a read key code resembles a pre-stored key code, the read key code is deemed authorized and the associated key can toggle the lock and where a read key code does not resemble (is different from) a pre-stored key code, the key is deemed unauthorized and denied access to the lock.

The Examiner concedes that Castleman, *et al.* simply ***compares*** a read key code with pre-stored authorized key codes to determine whether the read key code is an authorized code (it matches a pre-stored code) or not (it doesn't match any pre-stored code), but he asserts that this comparison is synonymous to analyzing electronic key data as recited in the subject claims. However, comparing key codes as disclosed in Castleman, *et al.* is ***not*** synonymous with analyzing electronic key data as recited in the subject claims. As defined in Merriam-Webster's online dictionary, the infinitive "to compare" means "to examine the character or qualities of especially in order to discover resemblances or differences." (http://www.merriam-webster.com). Thus, with comparing entities, the goal is to decipher whether the entities resemble or differ from one other, which is precisely what Castleman, *et al.* attempts to accomplish by comparing key codes. Synonyms of compare include contrast and collate. (http://www.merriam-webster.com). In contrast, the definition of the infinitive "to analyze" is "to study or determine the nature and relationship of the parts of by analysis," wherein "analysis" is a "separation of a whole into its component parts." (http://www.merriam-webster.com). Synonyms of analyze include dissect and breakdown. (http://www.merriam-webster.com).

In light of the Castleman, *et al.* and the dictionary definitions of the terms compare and analyze, it is readily apparent that Castleman, *et al.* does not disclose analyzing electronic key data as recited in the subject claims.

In addition, the Examiner relies on an incorrect interpretation of the term "comparison" to read, *via* inherency, a data analyzer into Castleman, *et al.* Specifically, the Examiner states that

since key codes are compared, an analysis is performed and, therefore, such comparison is *inherently* performed by a data analyzer. (Final Office Action, No. 5, p.4). However, this interpretation of compare and analyze is inconsistent with the dictionary definitions; the definitions clearly illustrate that compare and analyze are ***not*** synonyms, and, therefore, the *inherency* conclusion drawn by the Examiner is erroneous. "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749 (Fed. Cir. 1991). The fact that a characteristic may be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was [not] based on ... what was necessarily present in the prior art). Since Castleman, *et al.* does not disclose analyzing data, as recited in the subject claims, but instead discloses comparing key codes, the missing descriptive matter (a data adapter that analyzes electronic key data) is ***not*** necessarily present and would not be recognized by persons of ordinary skill in the relevant art. Thus, contrary to the Examiner's contention, Castleman, *et al.* does not disclose, expressly or inherently, a data analyzer as recited in the subject claims. Moreover, since Castleman, *et al.* does not disclose a data analyzer or analyzing electronic data, Castleman, *et al.* cannot disclose utilizing such analysis to generate control data that controls dangerous equipment, as recited in the subject claims.

In view of the foregoing, it is respectfully requested that this rejection of claims 1-3, 5-11 and 13-34 be withdrawn.

B. Rejection of Claims 4 and 12 Under 35 U.S.C. §103(a)

Claims 4 and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Castleman, *et al.* (US 5,508,691) in view of Mabuchi, *et al.* (US 6,417,760). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Castleman, *et al.* and Mabuchi, *et al.*, individually or in combination, do not teach or suggest all limitations of the subject claims.

i. *Applicable law*

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

ii. ***The combination of Castleman, et al. and Mabuchi, et al. does not teach or suggest all the claim limitations; thus, Castleman, et al. in view of Mabuchi, et al. does not make obvious the subject claims.***

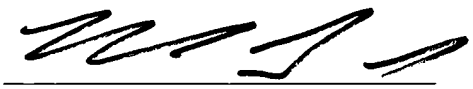
Claims 4 and 12 depend from independent claim 1, and Mabuchi *et al.* fails to make up for the aforementioned deficiencies of Castleman, *et al.* regarding analyzing electronic key data obtained from an electronic key with a data analyzer and employing the analysis to generate data to control dangerous equipment. Instead, Mabuchi *et al.* discloses an apparatus for inspecting target equipment and displaying the inspection information. Accordingly, this rejection should be withdrawn.

IX. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejection of claims 1-34 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063.

Respectfully submitted,
AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24th Floor, National City Center
1900 East 9th Street
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

Appendix of Claims (37 C.F.R. §1.192(c)(9))

1. A system that electronically controls a physical operation of dangerous equipment comprising:

an electronic key that stores electronic key data;

an electronic key reader that reads the electronic key data from the electronic key;

an electronic key data analyzer that is associated with the electronic key reader, the electronic key data analyzer analyzes the read electronic key data and generates a disconnect control data based, at least in part, on the electronic key data; and

a disconnector that is associated with the electronic key data analyzer and the dangerous equipment, the disconnector disables and re-enables operation of the dangerous equipment, based at least in part on the disconnect control data.

2. The system of claim 1, the disconnector further disables operation of the equipment based on a physical lock.

3. The system of claim 1, the electronic key reader further performs at least one of logging electronic key data, logging times when the operation of the piece of dangerous equipment is disabled, logging times when the operation of the piece of dangerous equipment is enabled, logging electronic key holder medical information, logging electronic key holder tasks, logging electronic key holder identity, scheduling dangerous equipment operation, scheduling related equipment operation and performing electronic data interchange.

4. The system of claim 1, further comprising a display, the display presents information related to at least one of technical manual data, schedule data, equipment identification data, equipment status information and safety manual data.

5. The system of claim 1, the electronic key data comprises at least one of key identifying information, key holder identity information, key holder medical information, key holder equipment access permissions, key holder equipment qualifications, key holder supervisor contact information, key holder security information and key holder task.

6. (Currently amended) The system of claim 1, the electronic key reader obtains the electronic key data *via* at least one of reading a magnetic strip on an electronic key inserted in the electronic key reader, receiving a radio frequency signal from an electronic key in transmission range of the electronic key reader and reading digital data from an integrated circuit memory chip on an electronic key.

7. The system of claim 1, the disconnector controls the flow of at least one of electricity, air, water and hydraulic fluid to the dangerous equipment.

8. The system of claim 1, further comprising a computer network, the computer network is coupled to one or more electronic key readers, one or more electronic key data analyzers, one or more disconnectors and one or more pieces of dangerous equipment, the computer network conveys a signal between one or more of the electronic key readers, the electronic key data analyzers, the disconnectors and the dangerous equipment.

9. The system of claim 8, the signal comprises at least one of electronic key data, electronic key data analysis data, equipment data and disconnect control data.

10. The system of claim 8, further comprising one or more additional disconnectors that disable operation of one or more additional pieces of dangerous equipment based on a physical lock.

11. The system of claim 8, the electronic key reader further performs at least one of logging electronic key data, logging times when the operation of the piece of dangerous equipment is disabled, logging times when the operation of the piece of dangerous equipment is enabled, logging electronic key holder medical information, logging electronic key holder tasks, logging electronic key holder identity, scheduling dangerous equipment operation, scheduling related equipment operation and performing electronic data interchange.

12. The system of claim 8, further comprising a display, the display presents at least one of technical manual data, schedule data, equipment identification data, equipment status information and safety manual data.

13. The system of claim 8, the electronic key data comprises at least one of key identifying information, key holder identity information, key holder medical information, key holder equipment access permissions, key holder equipment qualifications, key holder supervisor contact information, key holder security information and key holder task.

14. The system of claim 8, the electronic key reader obtains the electronic key data *via* at least one of reading a magnetic strip on an electronic key inserted in the electronic key reader, receiving a radio frequency signal from an electronic key in transmission range of the electronic key reader and reading digital data from an integrated circuit memory chip on an electronic key.

15. The system of claim 8, the disconnector prevents the flow of at least one of electricity, air, water and hydraulic fluid to the dangerous equipment.

16. The system of claim 15, further comprising a central station interfaced with the computer network, the central station that disables the operation of one or more pieces of dangerous equipment and re-enables the operation of one or more pieces of dangerous equipment, based, at least in part, on one or more pieces of electronic key data and/or one or more pieces of disconnect control data.

17. The system of claim 16, the central station performs at least one of logging electronic key data, logging times when the operation of one or more pieces of dangerous equipment is disabled, logging times when the operation of one or more pieces of dangerous equipment is enabled, logging electronic key holder medical information, logging electronic key holder tasks, logging electronic key holder identities, scheduling dangerous equipment operation, scheduling related equipment operation and performing electronic data interchange.

18. A computer readable medium that stores computer executable components of a system that electronically controls a physical operation of dangerous equipment, the system comprising:

an electronic key reading component that reads electronic key data from an electronic key;

an electronic key data analyzing component that analyzes the electronic key data and produces a disconnect control data; and

a disconnecting component that disables and re-enables the operation of a piece of dangerous equipment, based at least in part on the disconnect control data.

19. The computer readable medium of claim 18, further comprising a logging component that logs information concerning at least one of the electronic key data, the electronic key reading component, the electronic key data analyzing component, the disconnect control data and the disconnecting component.

20. The computer readable medium of claim 19, further comprising a scheduling component that schedules the operation of one or more pieces of dangerous equipment.

21. The computer readable medium of claim 20 further comprising an EDI component that performs electronic data interchange.

22. The computer readable medium of claim 21 further comprising a central station component that performs at least one of logging, scheduling and EDI for one or more electronic key reading components, electronic key data analyzing components and disconnecting components.

23. A data packet adapted to be transmitted from a first computer process to a second computer process, comprising:

disconnect data related to at least one of disabling and re-enabling one or more pieces of dangerous equipment, the disconnect data generated by a key analyzer in response to analysis performed on one or more pieces of electronic key data read from an electronic key by an electronic key reader.

24. A method that electronically controls a physical operation of dangerous equipment comprising:

collecting electronic key data;

obtaining a status of the dangerous equipment;

locally analyzing the electronic key data and producing disconnect data based, at least in part, on the analysis of the electronic key data and the status of the dangerous equipment; and

locally controlling the operation of the dangerous equipment based, at least in part, on the disconnect data.

25. The method of claim 24, further comprising:

locally logging data associated with at least one of the collected electronic key data, the disconnect data and the dangerous equipment operation.

26. The method of claim 25, further comprising:

locally scheduling the operation of one or more pieces of dangerous equipment based, at least in part, on at least one of the logged data, the electronic key data and the disconnect data.

27. The method of claim 26, further comprising locally engaging in or more electronic data interchanges.

28. The method of claim 24 further comprising locally displaying at least one of technical manual data, schedule data, equipment identification data, equipment status information and safety manual data.

29. A method that electronically controls a physical operation of dangerous equipment comprising:

collecting electronic key data;

centrally analyzing the electronic key data to produce disconnect data based, at least in part, on at least one of the electronic key data, a status of one or more pieces of dangerous equipment, a status of one or more pieces of related equipment and an identity of the dangerous equipment; and

centrally controlling the operation of at least one of one or more pieces of dangerous equipment and one or more pieces of related equipment based, at least in part, on the disconnect data.

30. The method of claim 29, further comprising:

centrally logging data associated with at least one of the collected electronic key data, the disconnect data and the dangerous equipment operation.

31. The method of claim 30, further comprising:

centrally scheduling the operation of at least one of one or more pieces of dangerous equipment and one or more pieces of related equipment based, at least in part, on at least one of the logged data, the electronic key data and the disconnect data.

32. The method of claim 31, further comprising centrally engaging in or more electronic data interchanges.

33. The method of claim 32, further comprising centrally displaying at least one of technical manual data, schedule data, equipment identification data, equipment status information and safety manual data.

34. A system that electronically controls a physical operation of dangerous equipment comprising:

means for reading electronic key data from an electronic key;

means for analyzing the electronic key data;

means for producing disconnect control data based, at least in part, on the electronic key data; and

means for disabling and re-enabling operation of the dangerous equipment, based at least in part on the disconnect control data.